ABSTRACT OF THE DISCLOSURE

Apparatus for monitoring operation of a processing system includes a set of modules for monitoring operation of a set of system primitives that allocate or release the system resources and are used by different processes running on the system. Preferably, the modules include at least one application knowledge module tracking the processes running on the system and monitoring the resources used thereby, a network knowledge module monitoring connections by the processes running on the system, a file-system analysis module monitoring the file-related operations performed within the system, and a device monitoring module monitoring operation of commonly used modules with the system. A preferred field of application is in host-based intrusion detection systems.